UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/436,135	11/09/1999	DAVID VAN GUNTER	200310	6185

7590 10/14/2003

LEYDIG VOIT & MAYER LTD
TWO PRUDENTIAL PLAZA
SUITE 4900
180 NORTH STETSON
CHICAGO, IL 606016780

EXAMINER	
SHIN, KYUNG H	

ART UNIT	PAPER NUMBER
2132	3

DATE MAILED: 10/14/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/436,135	VAN GUNTER ET AL.	
	Examiner	Art Unit	
	Kyung H Shin	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 November 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 1999* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: registry 86 (Fig. 1) referred to on page 13 line 7. A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 14 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 14 as a dependent claim recites the limitation "**the** pre-selected packet", which is not found in claim 8. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claim 1 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Jain** et al, U.S. Patent No. 6,311,218 in view of **Goldman** et al, U.S. Patent No. 5,684,951.

In regard to independent **claim 1,** Jain discloses authentication of a user on a node prior to allowing the user to send or receive data on a network (see col. 1, line 60) from a client computer as End System (ES) that can represent end-user (see col. 3, line 40, 41) data processing equipment as Personal computers (see col. 3, line 46) on Local Area Network (LAN). Jain discloses steps of:

- detecting a network port connection from a client (see col. 4, line 56) on end system;
- composing a challenge for user authentication (see col. 2, line 2) associate with network connection (see col. 1, line 64), and "encrypting with a private key" (see col. 6, line 12);

- transmitting the challenge (see col. 2, line 45);
- receiving a response (see col. 2, line 46);
- "decrypting with a public key" (see col. 6, line 14);
- receiving network data (see col. 1, line 60) through a network connection

It is noted that Jain does not teach obtaining the Message Digest (MD) value based on the challenge by decrypting the response; the calculations in order to obtain a MD value; and comparing the MD values. However, Goldman discloses:

- generating a validation key (see col. 9, line 7) utilizing a well-known MD5 Hash function, also referred to as a MD function, (see col. 9, line 14-16);
- calculating the MD value of the key, the user entered validation value (see col. 9, line 42);
- comparison (see Fig. 9) between the two MD values (see col. 10, line 52, 53), whether a match is found.

It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the inventions of Jain and Goldman that encrypting the challenge procedure of Jain to incorporate MD values from hash function for a calculation (see col. 9, line 14, 15) and comparison of values (see col. 10, line 52, 53), then match MD values from a hash function as taught in Goldman. One of ordinary skill in the art would have been motivated to add the invention of Goldman with cryptographic functions

utilizing a hash function (see col. 9, line 16) in order to secure user authentication through a network connection.

In regard to independent **Claim 8,** Jain discloses a method of authenticating a user (see col.2, line 33) in Challenge-Response scheme (see Fig 5), and verifies the identity of a user prior to allowing the user to send or receive data (see col.1, line 60).

- detecting a network connection (see col. 4, line 20) is disclosed in Jain for transmitting data (see col. 4, line 21);
- receiving (see col. 2, line 56) from the end system network data transmitted through the network connection;
- obtaining a user ID and a public key (see col. 4, line 27, 36);
- composing a challenge for a user authentication, and encrypting with a private key (see col. 6, line 12);
- sending the challenge (see col. 2, line 45) as directed to a method for encryption algorithm;
- decrypting the challenge with a public key (see col. 6, line 14); encrypting with a private key of the user (see col. 6,line 12) to create a response;
- sending the response to the policy agent (see col. 6, line 6);
- decrypting (see col. 6, line 14) the response;

It is noted that Jain does not disclose using a client computer on a network transmit network data through "a policy agent "; the calculations of cryptographic in order to obtain a Message Digest value; and comparing the two message digest values to determine whether there is a match there between. However, Goldman discloses:

- generating a first MD value (see col. 9, line 14) based on the challenge and the network data of the user;
- calculating (see col. 9, line 14, 15) a second MD value based on the challenge and the network data received through the network connection from the client computer;
- comparing (see col. 10, line 52, 53) the first and second MD values to determine whether there is a match between values.

It would have been obvious to one of ordinary skill in the art at the time the invention to modify Jain's encrypting the challenge procedure to incorporate with calculation (see col. 9, line 14, 15) and comparison of values (see col. 10, line 52, 53) to match message digests values from well-known hash function (Message Digest function) as taught in Goldman. One of ordinary skill in the art would have been motivated to substitute encryption/decryption with cryptographic functions utilizing the Hash function (see col. 9, line 16) in order to achieve strong security in user authentication over network.

Claim 2 and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain et al, U.S. Patent No. 6,311,218 in view of Goldman et al, U.S. Patent No. 5,684,951, and further in view of MacDoran et al. U.S. Patent No. 5,757,916.

Jain and Goldman do not disclose the policy agent is a firewall. However, MacDoran teaches that an authentication server software for secure network be a firewall of the network architecture (see col. 15, line 55) to perform the functions of a policy agent.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the policy agent role in Jain to implement a firewall as a security processor for a security entity (see col. 15, line 40) as taught in MacDoran. One of ordinary skill in the art would have been motivated to use a firewall in place of a policy agent to modify Jain, because the security policy implementation on network using a firewall is an effective safe guard to protect a network system in order to authenticate the client and data through the network connection.

Claim 3 - 7 and 9 - 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jain et al, U.S. Patent No. 6,311,218 in view of Goldman et al, U.S. Patent No. 5,684,951.

In regard to **claim 3 and 10** Jain discloses composing a challenge by "encryption with a public key" (see col. 5, line 44, 45) of the user.

In regard to **claim 4 and 11** Jain discloses, "decrypting with a private key" the response (see col. 6, line 5) to return it, and also encrypting with a public key (see col. 6, line 1) as claim 11 describes for the policy agent.

In regard to **claim 5 and 12** Jain discloses using the private key to encrypt the challenge (see col. 6, line 12), but Jain does not teach generating a 3rd MD value from data, and encrypting the 3rd MD value. However, Goldman discloses generation of the MD value with inclusion of the time value as "e.g., a coded timestamp" (see col. 9, line 36)

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention that calculating one more of hash value from data including a time value, then encrypted with the private key as taught in Goldman. One of ordinary skill in the art would have been motivated to generate 3rd MD value from network data with a hash function (see col. 9, line 16) in order to prevent unauthorized user accessing data from the network.

In regard to **claim 6 and 13** Jain discloses authentication process allowing data packets to be transmitted by user (see col. 9, line 16). But Jain does not disclose a form of packets for the received network data, and the calculation of the second MD value based on a pre-selected number of packets.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Jain's encrypting the challenge procedure to incorporate MD values

from a hash function for a calculation (see col. 9, line 14, 15) and comparison of hash values (see col. 10, line 52, 53), then match MD values from hash function as taught in Goldman. One of ordinary skill in the art would have been motivated to substitute encryption/decryption with cryptographic functions utilizing the hash function (see col. 9, line 16) in order to guarantee the authenticity and validity of network data.

In regard to **claim 7 and 9** Jain discloses according to the valid user ID after a match (see col. 10, line 54) occurs between two MD values. But Jain does not disclose having further executable instructions for performing access policies on the received network data.

It would have been obvious to one of ordinary skill in the art at the time of the invention to implement a procedure to perform specific functions after user validation, which was incorporated MD values then match the MD values from hash function as taught in Goldman. One of ordinary skill in the art would have been motivated to having further executable instructions for performing access policies (see col. 9, line 16) after the associated data received from network are ensured in order to allow further transmission of network data by a trusted authority.

In regard to **claim 14** Jain discloses the data decrypted from the challenge. Gordman discloses, wherein the step of the client computer generating the first MD value based on a random number, and data of the pre-selected packets (see col. 9, line 38, 41) of the received network data.

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention that calculating one more of hash encryption from data, which is encrypted with the private key of the policy agent, after generation of MD value based on a random number, data decrypted from the challenge, and data of the pre selected packets (see col. 9, line 39) as taught in Goldman for user authentication. One of ordinary skill in the art would have been motivated to substitute a detailed data packet form as an input to the hash function (see col. 9, line 38-41) using a principle of message digest function (see col.9, line 16) in order to compose the MD value including "time value" (see col. 9, line 14, 15) to modify Jain, because it prevents fraudulent data sending through network by improving the efficiency of the verification method for supporting the user to access network data.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. U.S. Patent No.5,745,573 to Lipner et al. discloses System and Method for Controlling Access to a User Secret.
b. U.S. Patent No.6,510,513 to Danieli discloses Security Services and Policy Enforcement for Electronic Data
c. U.S. Patent No.6,292,892 to Davis discloses Apparatus and Method for Providing Secured Communication

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305 - 0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-5447 for regular communications and 703-746-8360 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-2394.

Kyung H Shin
Examiner
Art Unit 2132

KHS
September 20, 2003

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100